(19)

Europäisches Patentamt

European Patent Office

Office européen des brevets

(11)   EP 0 809 402 B1

(12)   EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention
of the grant of the patent:
10.05.2000   Bulletin 2000/19

(51) Int Cl.⁷: **H04N 7/167**

(21) Application number: **97110364.3**

(22) Date of filing: **30.01.1991**

(54) External security module for a television signal decoder

Externes Sicherheitsmodul für einen Fernsehsignal-Decodierer

Module externe de sécurité pour un décodeur du signal de télévision

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IT LI LU NL SE

(30) Priority: **01.02.1990 US 473442**

(43) Date of publication of application:
26.11.1997   Bulletin 1997/48

(62) Document number(s) of the earlier application(s) in
accordance with Art. 76 EPC:
91904975.9 / 0 466 916

(73) Proprietor: **SCIENTIFIC-ATLANTA, INC.**
Atlanta, GA 30348 (US)

(72) Inventor: **Gammie, Keith Beverly**
Markham, Ontario L3P 1W1 (CA)

(74) Representative: **Kügele, Bernhard et al**
NOVAPAT INTERNATIONAL SA,
9, Rue du Valais
1202 Genève (CH)

(56) References cited:
EP-A- 0 343 805   WO-A-86/06240
WO-A-86/07724   US-A- 4 663 664

EP 0 809 402 B1

1   EP 0 809 402 B1   2

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates generally to the field of scrambling systems and more specifically, to an external security module for a television signal decoder of a broadcast, satellite, or cable television transmission system. The present invention has particular application for B-type Multiplexed Analog Component (B-MAC) satellite transmission, but may also be used for NTSC (National Television Standards Committee), PAL, SECAM, or proposed high definition television formats. In addition, the scrambling system of the present invention can be used in applications in related fields such as electronic banking networks, telephone switching systems, cellular telephone networks, computer networks, etc. The system has particular application to so-called "conditional-access" multichannel television systems, where the viewer may have access to several "basic" channels, one or more "premium" or extra-cost channels as well as "pay-per-view" programs.

2. Description of the Relevant Art

[0002] In a pay television system, a pay television service provider typically protects the signal from unauthorized subscribers and pirates through scrambling.

[0003] For the purposes of the following discussion and this invention, the term "subscriber" means one who is paying for the television service. The "subscriber" could thus be an individual consumer with a decoder in his own home, or could be a system operator such as a local cable TV operator, or a small network operator such as a Hotel/Motel operator with a central decoder for all televisions in the Hotel or Motel. In addition, the "subscriber" could be an industrial user, as described in U.S. Patent 4,866,770 assigned to the same assignee as the present application.

[0004] For the purposes of this invention, a network is defined as a program source, (such as a pay television provider), an encoder, (sometimes called a "head end"), a transmission means (satellite, cable, radio wave, etc.) and a series of decoders used by the subscribers as described above. A system is defined as a program source, an encoder, a transmission means, and a single receiving decoder. The system model is used to describe how an individual decoder in a network interacts with the encoder.

[0005] The scrambling process is accomplished via a key which may itself be encrypted. Each subscriber wishing to receive the signal is provided with a decoder having an identification number which is unique to the decoder. The decoder may be individually authorized with a key to descramble the scrambled signal, provided appropriate payments are made for service. Authoriza-

tion is accomplished by distributing descrambling algorithms which work in combination with the key (and other information) to paying subscribers, and by denying that information to non-subscribers and to all would-be pirates.

[0006] The key may be transmitted as a data signal embedded in the normal television transmission associated with the identification number of the decoder. In a typical television signal, there are so-called "vertical blanking intervals" (VBI) occurring in each field and "horizontal blanking intervals" (HBI) occurring in each line between the chrominance and luminance signals. Various other signals can be sent "in-band" in the vertical and horizontal blanking intervals including additional audio channels, data, and teletext messages. The key can be embedded in these "blanking intervals" as is well known in the art. Attention is drawn to U.S. Patent No. 4,829,569 assigned to the same assignee as the present application, showing how such data can be embedded in a B-MAC signal. Alternatively, the key may be sent "out-of-band" over a separate data channel or even over a telephone line.

[0007] Maintaining security in a conditional-access television network depends on the following requirements:

(i) The signal scrambling techniques must be sufficiently complex to insure that direct encryptographic attack is not practical.
(ii) keys distributed to an authorized decoder cannot be read out and transferred to other decoders.

[0008] The first condition can be satisfied by practical scrambling algorithms now available such as the DES (Data Encryption Standard) or related algorithms.

[0009] The second condition requires the physical security of certain devices within the television signal decoder and is much more difficult to satisfy. Such a device must prevent observation of both the key decryption process and the partially decrypted key signals.

[0010] Figure 1 shows a prior art conditional-access system for satellite transmission. In encoder 101, the source program information 102 which comprises video signals, audio signals, and data is scrambled in program scrambler 103 using a key from key memory 104. The scrambling techniques used may be any such techniques which are well known in the art. The key can be a signal or code number used in the scrambling process which is also required to "unlock" or descramble the program in program descrambler 108 in decoder 106. In practice, one key can be used (single layer encryption) or more than one key (not shown). The key is usually changed with time (i.e. - monthly) to discourage piracy. The scrambled programs and the key are transmitted through satellite link 105, and received by conditional-access decoder 106. Decoder 106 recovers the key from the received signal, stores it in key memory 107 and applies it to program descrambler 108 which de-

3   EP 0 809 402 B1   4

scrambles the scrambled program received over satellite link 105, and outputs unscrambled program 109. The system is not totally secure, as the key is transmitted in the clear through the channel and is available for recovery by pirates.

[0011]   To overcome this difficulty and referring to prior art Figure 2, a method of protecting the key during distribution is introduced into the system of Figure 1. Prior to transmission, the key used to scramble source program 202 in program scrambler 203 is recovered from key memory 204 and itself encrypted in key encryptor 210 using a secret serial number (SSN) from secret serial number database 211 which contains a list of the secret serial numbers of all legitimate subscribers. These secret serial numbers may relate to the unique identification numbers mentioned above for each decoder of a network of such decoders. The source program has now been scrambled using the key, and the key itself has been encrypted using a secret serial number. Thus, the key is not subject to compromise or recovery during transmission in comparison with the system of Figure 1. In order to descramble the program, the pirate must first obtain the secret serial number of a legitimate decoder, match it with the appropriately encrypted key, decrypt the key, and then descramble the program. The secret serial number is installed in decoder 206, for example, during manufacture in SSN memory 212 resident in decoder 206. The secret serial number is therefore unavailable to pirates provided that decoder 206 remains physically secure.

[0012]   Each secret serial number is unique to an individual decoder or, at least, unique to a group of decoders in order to be reasonably secure. The encrypted key may therefore be transmitted to each decoder individually by cycling through a database 211, containing all the secret serial numbers of the network in encoder 201 and forming a separate key distribution message in an addressed data packet individually addressed to each authorized decoder in the network. An individual decoder recognizes when its encrypted key has been received by reading the key distribution message attached to the encrypted key.

[0013]   In known B-MAC systems, the key is distributed in an addressed data packet individually addressed to a particular subscriber's decoder by means of its unique identification number. The addressed data packet is typically inserted in lines 4 through 8 of the vertical blanking interval. Each addressed data packet is typically addressed to one individual decoder. As there are sixty fields generated per second (30 frames of 2 interlaced fields each) in a B-MAC or NTSC television signal, at the rate of one addressed data packet per field, a possible sixty different decoders (or groups of decoders) can be addressed each second, or 3600 per minute, 215,000 per hour, and over 5 million per day. Since each decoder need only be addressed when the service level or encryption level changes, there are sufficient frames available to individually address each decoder even in

large systems. The address rate of the decoders may be increased by transmitting more than one addressed data packet per field. Additional data packets may be inserted in the vertical blanking interval or in the horizontal blanking intervals of each frame. The total number of possible addressable decoders is a function of the number on data bits available for decoder addresses. The B-MAC format typically uses 28 bits for decoder addresses, allowing for over 268 million possible decoder addresses. Attention is drawn to the United States Advanced Television Systems Committee Report T2/62, "MULTIPLEXED ANALOG COMPONENT TELEVISION BROADCAST SYSTEM PARAMETER SPECIFICATIONS", which describes the data format in a B-MAC signal.

[0014]   After receiving the addressed data packet, key decryptor 213 then decrypts the key using the secret serial number stored in SSN memory 212. If service to any decoder 206 in the network is to be terminated, the secret serial number for that decoder is simply deleted from SSN database 211, and decoder 206 is deauthorized at the beginning of the next key period.

[0015]   In a decoder such as the one shown in Figure 2, the pay television provider has to rely on the physical security of the decoder box itself to prevent a pirate from reading or modifying the secret serial number and key memories in the decoder or observing the key decryption process. In order to provide the necessary physical security, decoder boxes can be equipped with tamper-proof seals, specially headed screws and fasteners, or other tamper resistant packaging to make physical compromise of the decoder difficult. The subscriber Is aware that tampering with the decoder could alter the tamper-proof seals or damage the decoder and subsequent examination could lead to discovery.

[0016]   There are several disadvantages of relying on the physical security of the decoder to maintain system security. First, the pay television provider has to maintain ownership and control over all of the decoders of the network and then rent or lease the decoders to subscribers. The pay television provider is thus responsible for maintenance of all decoders and must maintain an expensive parts inventory and maintenance staff. In addition, in order to initiate service, a serviceperson must make a personal visit to the subscriber's location to install the decoder. In a pay television satellite system, such installation and service calls could be quite costly for remote installations which could be located anywhere in the world. Further, the physical security of a decoder could be breached without fear of discovery if a pirate could obtain a decoder that had been stolen either during the distribution process or from an individual subscriber's home.

[0017]   Hence, the system of Figure 2 can be secure only under the following conditions:

(i) It must be impossible to read or modify the SSN and key memories in the decoder.

(ii) It must be impossible to observe the key decryption process, or the links between the four elements (207, 208, 212, and 213) of the decoder.

[0018] One way to achieve both of these goals is by the use of a so-called "secure microprocessor".

[0019] Figure 3 shows a block diagram of a typical prior art microprocessor 320 with processor 321, program memory 322, memory address bus 328, memory data 326 and memory data bus 327. In such a device, input data 323 is processed according to a program stored in program memory 322, producing output data 324. Program memory 322 can be "read out" through memory data bus 327. That is, the memory can be stepped through by sequentially incrementing memory address 325 through memory address bus 328 into program memory 322. Output memory data 326 from memory data bus 327 will reveal the entire program contents of microprocessor 320, including any stored descrambling algorithm and secret serial number. With such data, a pirate can easily decrypt a key transmitted through satellite link 205 of Figure 2.

[0020] Figure 4 shows a block diagram of an ideal secure microprocessor 420 adapted for securing an algorithm and secret serial number according to one aspect of the present invention. The major difference between secure microprocessor 420 of Figure 4 and microprocessor 320 of Figure 3 is that both memory address bus 328 and memory data bus 327 are absent, so there is no way to step through program memory 422 for the purpose of reading or writing. Memory references are executed only by processor 421 according to its mask-programmed code which cannot be changed. All input data 423 is treated as data for processing, and all output data 424 is the result of processing input data 423. There is no mechanism for reading or modifying the contents of program memory 422 via the data inputs.

[0021] Modern devices are a close approximation to this ideal secure microprocessor. There is, however, one requirement which causes a variation from the ideal. Following manufacture, there must be a mechanism available to write into memory 422 the decoder specific secret serial number 430, as well as decryption algorithm 434. If this facility were available to a pirate, he could modify the secret serial number for the purpose of cloning. Therefore, this facility must be permanently disabled after the secret serial number has been entered.

[0022] A variety of techniques may be used to disable the facility for writing into the memory. Secure microprocessor 420 could be provided with on-chip fusible data links 431, a software lock, or similar means for enabling the secret serial number 430 and descrambling algorithm 434 to be loaded into memory 422 at manufacture. Then, for example, the fusible links shown in dashed lines are destroyed so that a pirate has no access to descrambling algorithm 434 or secret serial number 430 stored in program memory 422.

[0023] In an alternative embodiment, the microprocessor of Figure 4 can be secured with an "E^2 bit." The "E^2 bit", a form of software lock, will cause the entire memory (typically EEPROM) to be erased if an attempt is made to read out the contents of the memory. The "E^2 bit" provides two advantages; first, the memory is secured from would-be pirates, and second, the memory erasure will indicate that tampering has occurred.

[0024] A pirate would have to have access to extensive micro-chip facilities and a significant budget to compromise such a secure micro-processor. The physical security of the processor would have to be breached, destroying the processor and contents. However, integrated circuit technology continuously improves, and unexpected developments could occur which might enable attacks to be made at the microscopic level which are more economic than those available today. Further, the worldwide market for pirate decoders for satellite transmissions would provide the economic incentive to the increasingly sophisticated pirate electronics industry to compromise such a unit.

[0025] Copying a single decoder comprising a microprocessor according to Figure 4 could lead to decoder clones based on the single secret serial number in that single decoder. Discovery would result in the termination of that secret serial number, and thus termination of all of the clones. However, a pirate would also have the option of using the single compromised unit to recover the key. The pirate could then develop a decoder design which would accept the key as a direct input. These pirate units could then be illegally distributed to subscribers, who would pay the pirate for a monthly update of the key. The consequence of a security breach could become extremely damaging to the pay television provider.

[0026] Pay television providers are therefore at risk if security depends exclusively on the physical defenses of the secure microprocessor. Figure 5 shows a device which attempts to overcome the disadvantages of the devices of Figures 1 and 2 by providing a security device in a replaceable security module 514. Replaceable security module 514 comprises key decryptor 513, secret serial number memory 512 and key memory 507. As in Figure 2, encoder 501 scrambles source program 502 comprising video signals, audio signals and data in program scrambler 503 using a key from key memory 504. The key is encrypted in key encryptor 510 using a secret serial number (SSN) from secret serial number database 511 which contains a list of the secret serial numbers of all legitimate subscribers.

[0027] The same SSN is installed in secret serial number memory 512 in replaceable security module 514 which is removably attachable to decoder 506. Key decryptor 513 of replaceable security module 514 decrypts the key using the secret serial number stored in secret serial number memory 512. The decrypted key is then stored in key memory 507. Unlike Figure 2, the entire replaceable security module is removably at-

7   **EP 0 809 402 B1**   8

tached to decoder **506**. Program descrambler **508** reads the decrypted key from key memory **507** in replaceable security module **514** and uses the key to descramble and output descrambled program **509**. Removable security module **514** is designed to be replaced by the subscriber, preferably without any special tools and, thus, most conventionally may comprise a plug-in module.

[0028] The use of a plug-in module gives the pay television provider the ability to upgrade the technology in the security device by swapping it out at very low cost. In the event of a security breach, a new replaceable security module containing the program scrambling algorithm and SSN could be mailed out to authorized subscribers. The authorized subscribers could then remove the old replaceable security module from their decoder and insert the new replaceable security module themselves. System security is thus recovered without the expense of replacing the entire decoder or the expense of sending a service person to replace the replaceable security modules in each decoder. In addition, it is not necessary for the pay television provider to own the decoder itself: The decoder can be a generic commercially available unit purchased by the subscriber, or even integrated into the television itself. To initiate service, the pay television provider need only mail the replaceable security module to the subscriber and no service call is necessary.

[0029] Although the replaceable security module has the advantages of providing a guarantee that network security is recoverable following a breach, it also has some disadvantages. All the security resides in replaceable security module **514**, and decoder **506** itself is a generic unit. The key signal which is generated by replaceable security module **514** is observable at its transfer point to decoder **506**. The key can, however, be changed sufficiently often to ensure that it has no value to a potential pirate.

[0030] The problem with this approach is that a given removable security module **514** will operate with any decoder **506**, and that tampering with replaceable security module **514** does not involve damage to decoder **506**. Consequently, if replaceable security module **514** were to be compromised, piracy would become widespread very rapidly.

[0031] Although the devices as described above show a single key to scramble the program signal (so-called "single layer encryption") any of the prior art devices could also be practiced using a multiple key ("two layer", "three layer", etc.) scrambling system. Figure 6 shows an exam-pie of a prior art two layer encryption encoder **601**. Encoder **601** contains secret serial number database **611** which contains a list of secret serial numbers for all authorized subscribers. Key memory **604** stores the "Key of the Month" (KOM) which in this embodiment can be either an "even" key for even months (February, April, June, etc.) or an "odd" key for odd months (January, March, May, etc.). The key could also be different for each month of the year, or could be

made even more unique, depending on the available data bits for such a key. In addition, the key could be changed more frequently or less frequently than the monthly basis shown here.

[0032] Key encryptor **610** encrypts the key selected from key memory **604** and outputs a series of encrypted keys $E_{SSN}[KOM]$ each encrypted with a secret serial number from secret serial number database **611**, to data multiplexor **635**. Seed memory **636** contains a "seed" which is used for scrambling the audio and video signals. The "seed" can also be a data code or a signal similar to the key described above. Seed encryptor **637** encrypts the seed with the key of the month and outputs the encrypted seed $E_{KOM}[SEED]$ to data multiplexor **635**. Thus the key has been encrypted with the secret serial number, and the seed encrypted with the key. Neither the key nor the seed can be easily recovered during transmission.

[0033] In this embodiment, source program **602** comprises a Multiplexed Analog Video (MAC) signal **639** with the typical chrominance and luminance signals described previously, along with multiplexed audio data **638** which may comprise several different audio and non-audio (data) signals. For example, there may be at least two channels of audio (stereo) and additional channels of teletext for the hearing impaired. In addition, there may be additional channels of audio related to the video signal such as foreign language translations, unrelated audio signals such as radio programs or data signals such as subscriber messages, computer data, etc. All of these signals are digitized and multiplexed together, as is well known in the art, and the resulting multiplexed audio data **638** is then ready to be scrambled.

[0034] The seed passes through pseudo-random bit sequencer (PRBS) **643** and then is added to multiplexed audio data **638** in adder **644**. Together, pseudo-random bit sequencer (PRBS) **643** and adder **644** comprise a bit-by-bit encryptor **645** as is well known in the art. The resulting scrambled multiplexed audio data is then passed to data multiplexor **635** and is multiplexed with the encrypted seed and key.

[0035] MAC video signal **639** is scrambled in line translation scrambler **603** which scrambles the lines of the MAC signal using the "seed" from seed memory **636** for the scrambling algorithm. The resulting scrambled MAC signal is then sent to multiplexor **632** which multiplexes the scrambled MAC signal with the output from data multiplexor **635**. The multiplexed data output of data multiplexer **635** is modulated into pulse amplitude modulation (PAM) format by P.A.M. modulator **645**. The output B-MAC signal **646** contains MAC video signal **639** and multiplexed PAM audio data **638**, both scrambled with the seed, along with the seed encrypted with the key of the month, and a series of keys of the month which have been encrypted with the secret serial numbers of the subscriber's decoders, all multiplexed together.

[0036] In order to descramble the B-MAC signal **646**,

a pirate must be able to decrypt one of the encrypted keys, and use that key to decrypt the seed. However, as in the single layer encryption device described in Figure 2, the pirate only needs to compromise one of the decoders in order to obtain a secret serial number, and thus decrypt the key. With the key, a pirate can then decrypt the seed, and with the seed, descramble the program signal. Additional "layers" of encryption (i.e. - more seeds and keys) make pirating more cumbersome, as the pirate must decrypt more seeds and keys, however, once the first key has been decrypted, the subsequent keys and seeds can be decrypted as well. In embodiment shown in Figure 6, keys need be every other month (even months and odd months) for the pirate to be able to descramble the program signal all year. The secret serial numbers, seed, and key, as used in Figure 6, can be used effectively by the pay television provider to terminate a particular decoder by secret serial number and generally discourage piracy by amateurs. However, while this system has not yet been compromised, a determined pirate may comprise such a multi-layered encryption system with the aid of a compromised decoder, the heart of such piracy being the gaining of access to a secret serial number.

[0037]   EP0343805 discloses a decoder which decrypts a once-encrypted key in order to generate a working key which is used for descrambling a program signal. WO8606240 discloses a decoder with a removable plastic card comprising electronic circuitry. Decryption of a key is only possible when the card is connected to the decoder. The combined decoding logic in the decoder and the card operates so that the received signal is decoded and unscrambled. US4663664 discloses a removable electronic ticket for descrambling a transmitted video program. At least a portion of a descrambling circuit is formed on a substrate.

[0038]   In view of the deficiencies of the above prior art devices, it still remains a requirement in the art to provide a scrambling system for pay television systems which does not rely solely on the physical security of the decoder components to maintain system integrity.

Summary of the invention

[0039]   The invention in its various aspects is defined in the claims to which reference should now be made. Preferred features are laid out in the sub-claims.

[0040]   The present invention preferably provides a decoder with the features of appended claims 1 and 7 and a decoding method having the features of appended claims 13 and 19.

[0041]   Many of the above-stated problems and related problems of the prior art encryption devices have been solved by the principles of the present invention. The double-encryption technique discourages copying the replaceable security module, as each replaceable security module will work only with its mating decoder. The system also allows the replaceable security module

to be replaced following a system breach, thus allowing for recovery of system security.

[0042]   The system comprises an encoder for encoding a signal, the encoder further comprising a signal scrambler and a first and second key encrypters. The signal scrambler scrambles the signal and outputs a scrambled signal and a key for descrambling the scrambled signal. The first key encryptor is coupled to the signal scrambler and performs a first encyrption on the key using a first secret serial number and outputs a once-encrypted key. The second key encryptor is coupled to the first key encryptor and performs a further encryption on the once-encrypted key using a second secret serial number and outputs a twice-encrypted key.

[0043]   The system further comprises a transmitter coupled to the signal scrambler and the second key encryptor for transmitting the scrambled signal and twice-encrypted key.

[0044]   The system further comprises a decoder coupled to the transmitter for receiving and descrambling the scrambled signal. The decoder comprises first and second key decryptors and a descrambler. The first key decryptor is coupled to the transmitter and performs a first key decryption on the twice-encrypted key using the second secret serial number and outputs a partially decrypted key. The second key decryptor is coupled to the first key decryptor and perform a second key decryption on the partially decrypted key using the first secret serial number and outputs the decrypted key. The descrambler is coupled to the second key decryptor and the transmitter and descrambles the scrambled signal using the decrypted key and outputs the descrambled signal.

[0045]   In an alternative embodiment of the present invention, the decoder may function without the use of a replaceable security module. In the event of a system breach or a service level change, a replaceable security module may then be inserted into the decoder to "upgrade" the decoder.

[0046]   These and other objects and advantages of the invention, as well as the details of an illustrative embodiment, will be more fully understood from the following specification and drawings in which similar elements in different figures are assigned the same last two digits to their reference numeral (i.e., encoder 701 of Figure 7 and encoder 801 of Figure 8).

BRIEF DESCRIPTION OF THE DRAWINGS

[0047]   FIG. 1 shows an example of a prior art conditional-access system for satellite transmission with a key signal sent in the clear to the decoder.

[0048]   FIG. 2 shows an example of a prior art conditional-access system for satellite transmission using a single key encryption technique.

[0049]   FIG. 3 shows an example of a prior art microprocessor without a secure memory.

[0050]   FIG. 4 shows a secure microprocessor with a secure memory and fusible data links adapted for stor-

ing an algorithm and secret serial number according to the present invention.

[0051]   FIG. 5 shows an example of a conditional-access system for satellite transmission with a replaceable security module containing a first secret serial number.

[0052]   FIG. 6 shows another prior art conditional-access system for satellite transmission using an additional layer of encryption.

[0053]   FIG. 7 shows one exemplary embodiment of the conditional-access system of the present invention with an encoder encrypting the key with both a first and second secret serial number, a satellite transmission system, and a decoder containing a first secret serial number and a replaceable security module containing a second secret serial number.

[0054]   FIG. 8 shown another embodiment of the encryption system of the present invention including a multiplexor and demultiplexor for multiplexing the twice encrypted key with the scrambled program signal prior to transmission, and demultiplexing the twice encrypted key from the scrambled program signal after reception.

[0055]   FIG. 9 shows an alternative embodiment of the device of FIG. 7 incorporating a telephone controller for bi-directional telephone control for pay-per-view access or key transmission.

[0056]   FIG. 10 shows a block diagram of an alternative embodiment of the device of Figure 9, showing in detail how signals are passed between the decoder and the replaceable security module.

[0057]   FIG. 11 shows another embodiment of the device of FIG. 10 with the telephone controller, but without a replaceable security module.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0058]   Figure 7 shows the encryption system of the present invention comprising an encoder 701 for encoding a source program 702 for transmission over a satellite link 705 to a decoder 706. According to Figure 7, the key is encrypted and addressed to individual decoders, similar to the device in Figure 5. However, in this case, the key is encrypted not once, but twice and must also be decrypted twice in the decoder. The first decryption takes place in a replaceable security module 714 which is mounted on the exterior of the decoder 706, for example, as a plug-in module. The second decryption takes place in a fixed security element 719 which is an integral part of the decoder 706. Both decryptions must take place properly for the decoder to receive the key.

[0059]   The encoder 701 has a key memory 704 containing the key used to scramble program 702 in program scrambler 703. The key is first encrypted in first key encryptor 710 with a first secret serial number (SSN_0) stored in SSN_0 database 711. The key is further encrypted in second key encryptor 715 with a second secret serial number (SSN_1) from SSN_1 database 716. This produces a series of twice-encrypted keys which

are then transmitted along with the scrambled program via satellite link 705. The decoder 706 receives the encrypted program and one of the twice-encrypted keys and performs a first key decryption in replaceable security module 714. The replaceable security module 714 contains a second secret serial number (SSN_1), which could be assigned to a particular security module or series of modules, in SSN_1 memory 717. The replaceable security module 714 performs a first key decryption in first key decryptor 718 and outputs a partially decrypted key. The partially decrypted key, still unreadable to a pirate, is sent to second key decryptor 713 located in decoder 706 itself. There, the key is fully decrypted using the first secret serial number stored in SSN_0 memory 712. The fully decrypted key is now stored in key memory 707 and used to descramble the scrambled program received from satellite link 705 in program descrambler 708 and output descrambled program 709.

[0060]   Both replaceable security module 714 and an internal security element 719 of decoder 706 may be constructed according to the principles of Figure 4. For example, the second secret serial number SSN_1 may be loaded into SSN_1 memory 717 of Module 714 and fusible links used for loading the memory destroyed during manufacture. Similarly, SSN_0 memory 712 of internal security element 719 may be loaded during manufacture over a fusible link and the link destroyed. Also over a fusible link, algorithms may be loaded into key decryptors 718, 713 during manufacture and the fusible links subsequently destroyed

[0061]   The effect of twice-encrypting the key is to ensure that replaceable security module 714 must correspond to a particular decoder 706 and will not operate with any other decoder. Loss of replaceable security module 714 during distribution no longer presents a potential security breach. To compromise the system, it is now necessary to break the physical security of both replaceable security module 714 and internal security element 719. In order to fully compromise the system, the internal security element 719 must be attacked, restoring the risk to the subscriber that his decoder will be damaged.

[0062]   At the same time, the replaceable security module provides the pay television provider with the option of replacing system security by mailing out new replaceable security modules to all authorized subscribers. Returned replaceable security modules 714 could be re-used for a different subscriber decoder by reprogramming the SSN_0 and SSN_1 databases 711 and 716 to correspond to the combination of the first secret serial number of decoder 706 with the second secret serial number of security module 714. Alternatively, the returned replaceable security modules 714 could be destroyed, and a new replaceable security module 714 sent out, incorporating changes and improvements in the security technology to thwart potential pirates. In the event of a security breach, it is only necessary to replace the replaceable security module and not the complete

decoder in order to restore system security.

[0063]   Alternatively, the decoder **706** may function optionally without the use of the replaceable security module **717**. In such a system, encoder **701** may be programmed to perform single level key encryption by encrypting the key from key memory **704** once in second key encryptor **715**, bypassing first key encryptor **710**. Decoder **706** would sense the absence of removable security module **717** and perform only a single key decryption in second key decryptor **713**.

[0064]   If a system breach occurs, the pay television provider then mails out replaceable security modules to subscribers, uses the double encryption technique, and thus recovers system security. The optional usage of the replaceable security module has other attractive benefits as well. Subscribers who do not pay for any premium channels may not be sent a replaceable security module, as the "basic" channels may only use a once-encrypted key or may even be sent in the clear. If the subscriber wishes to upgrade to a premium channel or channels, the pay television provider may then mail that subscriber the appropriate replaceable security module.

[0065]   In addition, the replaceable security module may be used to add other additional features. Many cable television systems offer optional services such as IPPV (Impulse-Pay-Per-View) which require two-way communication between the decoder **706** and the head end. In the past, if a subscriber wished to upgrade to IPPV service, a subscriber's decoder would have to be altered by inserting a IPPV module internally or by adding an IPPV "side car" externally. Alternatively, the entire decoder would have to be replaced. All three options would necessitate a service call, causing inconvenience to the subscriber, and expense to the pay television provider. Similarly, when a pay television provider wishes to upgrade its entire encoder/decoder system, it must provide a new decoder to each subscriber which will work in the interim with both the old and new encoding techniques, as it is nearly impossible to replace all subscriber decoders simultaneously. Thus a decoder manufacturer is faced with the added expense of providing his state-of-the-art decoder with extra circuitry in order to function with the pay television provider's old encoder for the few months during the change over period.

[0066]   In both the above instances, the replaceable security module **714** may be used to upgrade the decoder **706** without the expense and inconvenience of a service call. The replaceable security module **714** may be mailed to the subscriber and the subscriber can then insert the replaceable security module **714** and instantly upgrade the decoder and add additional features (such as IPPV), alter the encoding technique, or providing an external level of security.

[0067]   The replaceable security module **714** may take one of several forms. In the preferred embodiment, the module may comprise a "smart card", a plastic "credit card" with a built-in micro-processor, such as described by the International Standards Organization in standard ISO 7816/1 and ISO7816/2. Attention is drawn on U.S. Patent No. 4,841,133 issued June 20, 1989, describing such a "smart card." The "smart card" may be equipped with a series of electrical contacts which connect to contacts in the decoder **706**. The contacts may provide power to the card, along with clock signals and data transmission.

[0068]   Figure 8 shows another embodiment of the present invention wherein the key is twice encrypted and addressed to individual decoders, similar to the device in Figure 7. The encoder **801** has a key memory **804** containing the key used to scramble program **802** in program scrambler **803**. The key is first encrypted in first key encryptor **810** with the first secret serial number (SSN_0) stored in SSN_0 database **811**. The key is further encrypted in second key encryptor **815** with a second secret serial number (SSN_1) from SSN_1 database **816**, producing a series of twice-encrypted keys as in Figure 7. However, in this embodiment, the twice encrypted keys are then multiplexed into the scrambled program in multiplexor **832** and transmitted via satellite link **805**.

[0069]   The decoder **806** receives the encrypted program and demultiplexes the twice encrypted keys from the scrambled program signal in demultiplexor **833**. The decoder **806** then chooses the proper twice encrypted key based on the key message associated with the proper key for that decoder, and performs a first key decryption in replaceable security module **814**. The partially decrypted key is then sent to second key decryptor **813** located in the decoder **806** itself. There, the key is fully decrypted using the unique first secret serial number stored in SSN_0 memory **812**. The fully decrypted key is now stored in key memory **807** and used to decrypt the program in the program descrambler **808** and output the decrypted program **809**. The second key decryptor **813**, key memory **807**, and SSN_0 memory **812** together comprise fixed internal security element **819**.

[0070]   Figure 9 shows an alternative embodiment of the present invention with a telephone controller. Decoder **906** is similar to the decoder **706** of Figure 7, except that decoder **906** of Figure 9 also includes a telephone controller **940** for receiving or sending an encrypted key or other data. Telephone controller **940** adds an additional level of security to the system, as the key does not have to be transmitted with the program signal over a separate channel as in Figure 7 or multiplexed into the signal as in Figure 8. In addition, the telephone controller **940** can provide two-way communication with the program source for such features as pay-per-view (PPV) or impulse pay-per-view (IPPV) programming.

[0071]   Pay-per-view programming is defined here as any programming where the subscriber can request authorization to watch a particular program. In many pay television systems, pay-per-view programming is used for sporting events (boxing, wrestling, etc.) which are not transmitted on a regular basis. A subscriber wishing to view the event must receive authorization in the form of a special descrambler mechanism, or in the form of a

special code transmitted or input to the subscriber's decoder. Some pay-per-view television systems allow the subscriber to request a pay-per-view program (i.e. - movies) to watch. The pay television provider then transmits the requested program and authorizes that subscriber's decoder to receive the signal

[0072] Impulse pay-per-view (IPPV) programming is defined here as any programming where the subscriber has a pre-authorized number of "credits" saved in his individual decoder. If a subscriber wishes to view a particular program, the subscriber merely actuates the decoder, the appropriate number of credits are subtracted from the subscriber's remaining credits, and the subscriber is immediately able to view the program.

[0073] In a pay-per-view embodiment of the present invention, the decoder may send a signal to the head end via the telephone controller 940 with a request for authorization to decode a pay-per-view program. Alternately, the decoder 906 may store authorization information (i.e.-credits) for pay-per-view programming, and forward actual pay-per-view data via the telephone controller 940 at a later time.

[0074] The telephone controller 940 could be a computer modem type device, or could work using touchtone signals to communicate with the head end. Preferably, the telephone controller is a modem type device, communicating with the head end using a TSK protocol. Attention is drawn to copending application Serial No. 187,978 filed April 29, 1988 describing TSK operation and published as US 4926444 on 15 May 1990. The pay television provider can thus send appropriate authorization information (TEL) to the subscriber, encrypted with the subscriber's secret telephone number (STN). The secret telephone number is not a telephone number in the ordinary sense, but rather another type of secret serial number, which could be assigned to a given telephone controller 940 or series of telephone controllers. Once received by the decoder 906, the authorization information may be used to enable descrambling of a particular pay-per-view program or programs.

[0075] In another embodiment, which could be used in conjunction with the pay-per-view embodiment described above, the telephone controller can he used to receive the key encrypted with the secret telephone number. The scrambled program signal 941 is input to the decoder 906 which provides the input signal 941 to a clock/data recovery unit 942 and the video/audio descrambler 908. The clock/data recovery unit 942 provides sync and data for the program signal fed to the fixed security element 919. Fixed security element 919 contains a key decryptor, key memory and SSN_0 memory. The telephone controller 940 receives the key, encrypted with the secret telephone number of the decoder (STN) stored in the replaceable security module 914. The telephone controller 940 typically commences communication and can be programmed to call the head end at a predetermined time or at a predetermined time interval, or upon receiving a signal from the head end pref-

erably when phone usage is at a minimum (i.e. - early morning hours). The telephone controller can call the head end via a toll free 1-800 number, a so-called "watts" line, or via a local call to a commercial data link such as TYMNET or TELENET. Once the call is connected and communications established, the decoder 906 uploads to the head end a record of pay-per-view usage encrypted with the secret telephone STN_1. The head end may then download data similarly encrypted to the decoder 906 including new keys, secret serial numbers, or decryption algorithms. The encrypted key may be sent to the fixed security element 919, which has removably attached thereto the replaceable security module 914. The key is then decrypted in the replaceable security module using the secret telephone number, and decoder control information is sent to the program descrambler 908 to produce the descrambled program 909.

[0076] As discussed above, a new secret serial number or decryption algorithm, encrypted with the secret telephone number, may be sent from the head end to a decoder through telephone controller 940. The encrypted secret serial number or decryption algorithm is then decrypted and stored in the replaceable security module. This downloading of decryption algorithms and secret serial numbers via the telephone controller 940 is sometimes called an "E^2 patch", and allows the pay television provider to maintain or recover system security by loading new information into a decoder's EEPROM. An E^2 patch does not necessarily entail changing the entire decryption algorithm in the decoder 906. The secret serial number or merely a portion of the decryption algorithm, such as a particular byte or data table need only be changed in order to sufficiently alter the decryption algorithm. The E^2 patch allows the pay television provider or upgrade the encryption system to fix "bugs" and recover system security.

[0077] After receiving a signal through the telephone controller 940, the head end will send an acknowledgment signal to the decoder, indicating that information has been received. Similarly, after data has been downloaded from the head end to the decoder through the telephone controller, the decoder will return an acknowledgment signal to the head end that data has been received.

[0078] In addition to pay-per-view requests or records, telephone controller 940 can also be used to upload other signals from the decoder. For example, tamper protection information such as described in connection with Figure 4 can be sent indicating whether or not the decoder has been tampered with. Further, program viewing information can be uploaded to the pay television provider for television rating purposes (i.e., - Nielson ratings)

[0079] In general, any data that can be delivered via the B-MAC input 941 of Figure 9 (or NTSC, PAL, SECAM, etc.) can also be downloaded through the telephone controller 940. Such information includes, but is

not limited to, blackout codes, tiering information, personal messages number of available credits, group identification numbers, and other system data. Generally, the telephone controller 940 is used for infrequent communications, such as periodic security level changes and IPPV requests, due to the limited bandwidth of telephone lines and the increased cost of sending information via telephone versus the B-MAC input.

[0080] The telephone information (TEL) encrypted with the secret telephone number (STN) remains encrypted throughout the decoder 906 and may only be decrypted in the replaceable security module 914. The decrypted telephone information does not pass out of the replaceable security module 914, in order to prevent observation by a pirate. In order for the decoder 906 to descramble a scrambled program, both the telephone information and the addressed data packet received through the B-MAC input 941 must be present. By relying on both information sources, piracy is virtually impossible, as the potential pirate must break into the pay television provider's telephone system as well as decrypt the twice-encrypted key.

[0081] Figure 10 shows a more detailed diagram of the device of Figure 9, showing how the various signals are sent between the fixed security element 1019 and the replaceable security module 1014. In this embodiment, both the fixed and replaceable security modules 1019 and 1014 are built around secure microprocessors 1050 and 1051 similar to that shown in Figure 4. In Figure 10, the subscript "0" is used to denote signals and keys stored or decrypted in the fixed security element 1019, while the subscript "1" denotes signals and keys stored or decrypted in the replaceable security module 1014.

[0082] Fixed security element 1019 comprises a secure microprocessor 1050 which receives signals 1053, 1054, and 1055 as inputs. Signal 1053 is the program (SYS) which has been scrambled with a key-of-the-month (KOM) and is represented by the symbol E_{KOM1} (SYS). Signal 1054 is the key-of-the-month (KOM) which has been twice-encrypted with the two secret serial numbers (SSN_0 and SSN_1) of the fixed and replaceable security modules 1019 and 1014, respectively and is represented by the symbol $E_{SSN0}(E_{SSN1}(KOM1))$.

[0083] Signal 1055 is an additional signal, E_{STN1} (TEL), which is the telephone data encrypted with a secret telephone number (STN) described in Figure 9 above. The telephone data can be used to provide an additional level of security, as well as to allow the subscriber to request "pay-per-view" programs via the phone line as described in Figure 9 above.

[0084] Secure microprocessor 1050 performs a first decryption of twice-encrypted key 1054 using the first secret serial number SSN_0 stored within secure microprocessor 1050. Secure microprocessor 1050 passes partially decrypted key-of-the-month $E_{SSN1}(KOM)$ 1061 to replaceable security module 1014 along with scrambled program E_{KOM1} (SYS) 1062 and encrypted telephone data E_{STN1} (TEL) 1060.

[0085] Replaceable security module 1014 comprises secure microprocessor 1051 which has secure memory 1052 where the second secret serial number SSN_1 is stored along with the secret telephone number STN_1, the encryption algorithm E, and other authorization information. Secure microprocessor 1051 performs a further decryption on partially decrypted key-of-the-month $E_{SSN1}(KOM)$ 1061 received from fixed security element 1019, using the second secret serial number SSN_1 and encryption algorithm E stored within secure memory 1052. The decrypted key-of-the-month (KOM1) is stored in the secure memory 1052 of secure microprocessor 1051. As discussed in Figure 4, secure memory 1052 cannot be directly addressed or read out, and as such the second secret serial number SSN_1 and the encryption algorithm E cannot be observed by a potential pirate.

[0086] Secure microprocessor 1051 also decrypts the telephone data (TEL) using the secret telephone number STN_1 stored within the secure memory 1052 of the secure microprocessor 1051. If the key-of-the-month (KOM1) can be decrypted, and authorization is present (for pay-per-view), or unnecessary (for other channels), then scrambled program E_{KOM1} (SYS) 1062 can be descrambled in replaceable security module 1014, producing decoder control information DCI_1 1058. Decoder control information DCI_1 1058 typically contains the line translation scrambling information for the video signal, and decryption information for the multiplexed audio data along with other information such as whether teletext is enabled and which audio channel is to be selected. The program control information DCI_1 1058 and the encrypted telephone data E_{STN1} (TEL) are sent to the fixed security element 1019. If authorization is present (for IPPV) or unnecessary (for other channels), the secure microprocessor 1050 outputs the program control data 1058 to the rest of the decoder (not shown) for program descrambling. On-screen display support information (OSD) 1057 is decoded from the encrypted program signal $EKOM_1$ (SYS) and provides information how on-screen display is controlled by fixed security element 1019 to display personal messages, control a barker channel, indicate the number of remaining credits, indicate authorized channels as well as other ways of controlling displayed information.

[0087] Figure 11 shows a further embodiment of the present invention, without replaceable security module. In this embodiment, the subscript "0" has been used to denote that all decryptions take place within secure microprocessor 1150. Decoder 1106 comprises secure microprocessor 1150 with secure memory 1152. Secure memory 1152 contains a secret serial number SSN_0 and a secret telephone number STN_0 unique to that decoder or a series of decoders loaded during manufacture and secured with an "E² bit" as discussed in connection with Figure 4. Scrambled program E_{KOM0} (SYS) 1153 and once-encrypted key-of-the-month $E_{SSN0}(KOM0)$ 1154

are input to decoder **1106** along with encrypted telephone data $E_{STN0}(TEL)$ **1155**.

[0088] Secure microprocessor **1150** decrypts encrypted telephone data $E_{STN0}(TEL)$ **1155** using the secret telephone number STN_0 stored in secure memory **1152**. The decrypted telephone data (TEL) is also stored in secure memory **1152** to prevent observation by pirates. The telephone data (TEL) may provide authorization information to decoder **1106** as to whether decoder **1106** is presently authorized to decrypt some or all of the received scrambled programs. In addition, other information may be transferred between the decoder and the head end as discussed in connection with Figure 9.

[0089] If authorization is present, secure microprocessor **1150** uses the first secret serial number SSN_0 stored in secure memory **1152** to decrypt the key KOM_0. As in Figure 10, the secure microprocessor **1150** then outputs program control information DCI_0 **1156** to the remainder of decoder **1106** in order to descramble the program signal.

Claims

1. A decoder comprising a fixed security element (719), the fixed security element including a processor (713) to process a once-encrypted key (1061) based on a key (SSN_0) to generate a working key (KOM1) and to process scrambled program data (1062) based on the working key to generate decoder control information (1058) useable for descrambling scrambled signals, the decoder further comprising a replaceable security module removably attachable to the decoder, the replaceable security module including a processor to process a twice-encrypted key based on a second key (SSN_1) to generate a partially-decrypted key, the processor of the fixed security element processing the partially-decrypted key as the once-encrypted key so that the working key is recovered from the twice-encrypted key.

2. A decoder according to claim 1, wherein the processor of the fixed security element comprises a secure processor with an internal memory to store the working key and configured so that the working key is unobservable.

3. A decoder according to claim 1 or claim 2, wherein the processor of the fixed security element comprises a secure processor with an internal memory to store the first key (SSN_0) and configured so that the first key is unobservable.

4. A decoder according to claim 1, 2 or 3, wherein the processor of the fixed security element is configured to generate successive decoder control information from successively processed scrambled

program data while the working key remains unchanged.

5. A decoder according to any of claims 1 to 4, wherein the processor of the replaceable security module comprises a secure processor with an internal memory to store the second key (SSN_1) and configured so that the second key is unobservable.

6. A decoder according to any of claims 1 to 5, wherein the decoder is a first decoder of a cable system, the cable system including at least one other decoder, each decoder of said at least one other decoder including an associated fixed security element, the replaceable security module of the first decoder being incapable of generating a once-encrypted key that can be processed by the fixed security element of any decoder of said at least one other decoder to generate the working key.

7. A decoder comprising a replaceable security module (1014), the replaceable security module including a processor (1051) to process a once-encrypted key (1061) based on a first key (SSN_0) to generate a working key (KOM1) and to process scrambled program data (1062) based on the working key to generate decoder control information (1058) useable for descrambling scrambled signals, the decoder further comprising a fixed security element, the fixed security element including a processor to process a twice-encrypted key based on a second key (SSN_1) to generate a partially-decrypted key, the processor of the replaceable security module processing the partially-decrypted key as the once-encrypted key so that the working key is recovered from the twice-encrypted key.

8. A decoder according to claim 7, wherein the processor of the replaceable security module comprises a secure processor with an internal memory to store the working key and configured so that the working key is unobservable.

9. A decoder according to claim 7 or 8, wherein the processor of the replaceable security module comprises a secure processor with an internal memory to store the first key (SSN_0) and configured so that the first key is unobservable.

10. A decoder according to claim 7, 8 or 9, wherein the processor of the replaceable security module is configured to generate successive decoder control information from successively processed scrambled program data while the working key remains unchanged.

11. A decoder according to any of claims 7 to 10, wherein the processor of the fixed security element com-

21   EP 0 809 402 B1   22

prises a secure processor with an internal memory to store the second key (SSN_1) and configured so that the second key is unobservable.

12. A decoder according to any of claims 7 to 11, wherein the decoder is a first decoder of a cable system, the cable system including at least one other decoder, each decoder of said at least one other decoder including an associated replaceable security module, the fixed security element of the first decoder being incapable of generating a once-encrypted key that can be processed by the replaceable security module of any decoder of said at least one decoder to generate the working key.

13. A decoding method in a decoder comprising steps of:

processing a twice-encrypted key in a processor of a removably attachable replaceable security module based on a first key (SSN_1) to generate a partially-decrypted key; processing of the partially-decrypted key in a processor of a fixed security element as a once-encrypted key (1061) based on a second key (SSN_0) to generate a working key (KOM1); and processing scrambled program data (1062) based on the working key to generate decoder control information (1058) useable for descrambling scrambled signals.

14. The decoding method of claim 13, further comprising a step of storing the working key in an internal memory of the processor of the fixed security element so that the working key is unobservable.

15. The decoding method of claim 13 or claim 14, further comprising a step of storing the second key (SSN_0) in an internal memory of the processor of the fixed security element so that the second key is unobservable.

16. The decoding method of any of claims 13 to 15, further comprising a step of storing the first key (SSN_1) in an internal memory of the processor of the replaceable security module so that the first key is unobservable.

17. The decoding method of any of claims 13 to 16, further comprising a step of storing the second key (SSN_0) in an internal memory of the processor of the fixed security element so that the second key is unobservable.

18. The decoding method of any of claims 13 to 17, wherein:

the fixed security element is a first fixed security

element of a cable system, the cable system including at least one other fixed security element; and the step of processing a twice-encrypted key generates the partially-decrypted key so that the partially-decrypted key cannot be processed as the once-encrypted key by any fixed security element of the at least one other fixed security element to generate the working key.

19. A decoding method in a decoder comprising steps of:

processing a twice-encrypted key in a processor of a fixed security element based on a first key (SSN_1) to generate a partially-decrypted key; processing the partially-decrypted key in a processor of a removably attachable replaceable security module as a once-encrypted key (1061) based on a second key (SSN_0) to generate a working key (KOM1); and processing scrambled program data (1062) based on the working key to generate decoder control information (1058) useable for descrambling scrambled signals.

20. The decoding method of claim 19, further comprising a step of storing the working key in an internal memory of the processor of the replaceable security module so that the working key is unobservable.

21. The decoding method of claim 19 or claim 20, further comprising a step of storing the second key (SSN_0) in an internal memory of the processor of the replaceable security module so that the second key is unobservable.

22. The decoding method of any of claims 19 to 21, further comprising a step of storing the first key (SSN_1) in an internal memory of the processor of the fixed security element so that the first key is unobservable.

23. The decoding method of any of claims 19 to 22, further comprising a step of storing the second key (SSN_0) in an internal memory of the processor of the replaceable security module so that the second key is unobservable.

24. The decoding method of any of claims 19 to 23, wherein:

the replaceable security module is a first replaceable security module of a cable system, the cable system including at least one other replaceable security module; and the step of processing the twice-encrypted key

23　　　　　　　　EP 0 809 402 B1　　　　　　　24

generates the partially-decrypted key so that the partially-decrypted key cannot be processed as the once-encrypted key by any replaceable security module of the at least one other replaceable security module to generate the working key.

25. The decoding method of any of claims 13 to 24, further comprising a step of repeating the step of processing scrambled program data to generate successive decoder control information from successively processed scrambled program data while the working key remains unchanged.

Patentansprüche

1. Ein Decodierer mit

einem festen Sicherheitselement (719), wobei das feste Sicherheitselement einen Prozessor (713) aufweist, um einen einfach chiffrierten Codeschlüssel (1061) auf der Grundlage eines Codeschlüssels (SSN_0) zu verarbeiten, um einen Arbeits-Codeschlüssel (KOM1) zu erzeugen und verschlüsselte Programmdaten (1062) auf der Grundlage des Arbeits-Codeschlüssels zu verarbeiten, um Decodierer-Kontrollinformationen (1058), die zum Entschlüsseln von verschlüsselten Signalen verwendet werden können, zu erzeugen, und einem austauschbaren Sicherheitsmodul, das abnehmbar am Decodierer angebracht ist, wobei das austauschbare Sicherheitsmodul einen Prozessor aufweist, um einen zweifach chiffrierten Codeschlüssel auf der Grundlage eines zweiten Codeschlüssels (SSN_1) zu verarbeiten, um einen teildechiffrierten Codeschlüssel zu erzeugen, wobei der Prozessor des festen Sicherheitselements den teildechiffrierten Codeschlüssel als einfach chiffrierten Codeschlüssel verarbeitet, sodass der Arbeits-Codeschlüssel aus dem zweifach chiffrierten Codeschlüssel regeneriert wird.

2. Decodierer nach Anspruch 1, dadurch gekennzeichnet, dass der Prozessor des festen Sicherheitselements einen sicheren Prozessor mit einem internen Speicher zum Speichern des Arbeits-Codeschlüssels aufweist und so gestaltet ist, dass der Arbeits-Codeschlüssel nicht beobachtet werden kann.

3. Decodierer nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Prozessor des festen Sicherheitselements einen sicheren Prozessor mit einem internen Speicher zum Speichern des ersten Codeschlüssels (SSN_0) aufweist und so gestaltet

ist, dass der erste Codeschlüssel nicht beobachtet werden kann.

4. Decodierer nach Anspruch 1, 2 oder 3, dadurch gekennzeichnet, dass der Prozessor des festen Sicherheitselements so gestaltet ist, dass er aufeinander folgende Decodierer-Kontrollinformationen aus fortlaufend verarbeiteten verschlüsselten Programmdaten erzeugt, während der Arbeits-Codeschlüssel unverändert bleibt.

5. Decodierer nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Prozessor des austauschbaren Sicherheitsmoduls einen sicheren Prozessor mit einem internen Speicher zum Speichern des zweiten Codeschlüssels (SSN_1) aufweist und so gestaltet ist, dass der zweite Codeschlüssel nicht beobachtet werden kann.

6. Decodierer nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass der Decodierer ein erster Decodierer eines Kabelnetzes ist, wobei das Kabelnetz mindestens einen weiteren Decodierer aufweist, wobei jeder Decodierer von dem mindestens einen weiteren Decodierer ein zugehöriges festes Sicherheitselement aufweist, wobei das austauschbare Sicherheitsmodul des ersten Decodierers keinen einfach chiffrierten Codeschlüssel erzeugen kann, der vom festen Sicherheitselement eines Decodierers von dem mindestens einen weiteren Decodierer verarbeitet werden kann, um den Arbeits-Codeschlüssel zu erzeugen.

7. Ein Decodierer mit

einem austauschbaren Sicherheitsmodul (1014), wobei das austauschbare Sicherheitsmodul einen Prozessor (1051) aufweist, um einen einfach chiffrierten Codeschlüssel (1061) auf der Grundlage eines ersten Codeschlüssels (SSN_0) zu verarbeiten, um einen Arbeits-Codeschlüssel (KOM1) zu erzeugen und verschlüsselte Programmdaten (1062) auf der Grundlage des Arbeits-Codeschlüssels zu verarbeiten, um Decodierer-Kontrollinformationen (1058), die zum Entschlüsseln von verschlüsselten Signalen verwendet werden können, zu erzeugen, und einem festen Sicherheitselement, wobei das feste Sicherheitselement einen Prozessor aufweist, um einen zweifach chiffrierten Codeschlüssel auf der Grundlage eines zweiten Codeschlüssels (SSN_1) zu verarbeiten, um einen teildechiffrierten Codeschlüssel zu erzeugen, wobei der Prozessor des austauschbaren Sicherheitsmoduls den teildechiffrierten Codeschlüssel als einfach chiffrierten Codeschlüssel verarbeitet, sodass der Arbeits-Code-

25   **EP 0 809 402 B1**   26

schlüssel aus dem zweifach chiffrierten Code-
schlüssel regeneriert wird.

8. Decodierer nach Anspruch 7, dadurch gekenn-
zeichnet, dass der Prozessor des austauschbaren
Sicherheitsmoduls einen sicheren Prozessor mit ei-
nem internen Speicher zum Speichern des Arbeits-
Codeschlüssels aufweist und so gestaltet ist, dass
der Arbeits-Codeschlüssel nicht beobachtet wer-
den kann.

9. Decodierer nach Anspruch 7 oder 8, dadurch ge-
kennzeichnet, dass der Prozessor des austausch-
baren Sicherheitsmoduls einen sicheren Prozessor
mit einem internen Speicher zum Speichern des er-
sten Codeschlüssels (SSN_0) aufweist und so ge-
staltet ist, dass der erste Codeschlüssel nicht be-
obachtet werden kann.

10. Decodierer nach Anspruch 7, 8 oder 9, dadurch ge-
kennzeichnet, dass der Prozessor des austausch-
baren Sicherheitsmoduls so gestaltet ist, dass er
aufeinander folgende Decodierer-Kontrollinforma-
tionen aus fortlaufend verarbeiteten verschlüssel-
ten Programmdaten erzeugt, während der Arbeits-
Codeschlüssel unverändert bleibt.

11. Decodierer nach einem der Ansprüche 7 bis 10, da-
durch gekennzeichnet, dass der Prozessor des fe-
sten Sicherheitselements einen sicheren Prozes-
sor mit einem internen Speicher zum Speichern des
zweiten Codeschlüssels (SSN_1) aufweist und so
gestaltet ist, dass der zweite Codeschlüssel nicht
beobachtet werden kann.

12. Decodierer nach einem der Ansprüche 7 bis 11, da-
durch gekennzeichnet, dass der Decodierer ein er-
ster Decodierer eines Kabelnetzes ist, wobei das
Kabelnetz mindestens einen weiteren Decodierer
aufweist, wobei jeder Decodierer von dem minde-
stens einen weiteren Decodierer ein zugehöriges
austauschbares Sicherheitsmodul aufweist, wobei
das feste Sicherheitselement des ersten Decodie-
rers keinen einfach chiffrierten Codeschlüssel er-
zeugen kann, der vom austauschbaren Sicherheits-
modul eines Decodierers von dem mindestens ei-
nen weiteren Decodierer verarbeitet werden kann,
um den Arbeits-Codeschlüssel zu erzeugen.

13. Ein Decodierungsverfahren in einem Decodierer
mit den Schritten

Verarbeiten eines zweifach chiffrierten Code-
schlüssels in einem Prozessor eines aus-
tauschbaren Sicherheitsmoduls, das abnehm-
bar angebracht werden kann, auf der Grundla-
ge eines ersten Codeschlüssels (SSN_1), um ei-
nen teildechiffrierten Codeschlüssel zu erzeu-

gen;
Verarbeiten des teildechiffrierten Codeschlüs-
sels in einem Prozessor eines festen Sicher-
heitselements als einfach chiffrierter Code-
schlüssel (1061) auf der Grundlage eines zwei-
ten Codeschlüssels (SSN_0), um einen Arbeits-
Codeschlüssel (KOM1) zu erzeugen; und
Verarbeiten von verschlüsselten Programmda-
ten (1062) auf der Grundlage des Arbeits-Co-
deschlüssels, um Decodierer-Kontrollinforma-
tionen (1058) zu erzeugen, die zum Entschlüs-
seln von verschlüsselten Signalen verwendet
werden können.

14. Decodierungsverfahren nach Anspruch 13, das au-
ßerdem einen Schritt des Speicherns des Arbeits-
Codeschlüssels in einem internen Speicher des
Prozessors des festen Sicherheitselements auf-
weist, sodass der Arbeits-Codeschlüssel nicht be-
obachtet werden kann.

15. Decodierungsverfahren nach Anspruch 13 oder 14,
das außerdem einen Schritt des Speicherns des
zweiten Codeschlüssels (SSN_1) in einem internen
Speicher des Prozessors des festen Sicherheits-
elements aufweist, sodass der zweite Codeschlüs-
sel nicht beobachtet werden kann.

16. Decodierungsverfahren nach einem der Ansprüche
13 bis 15, das außerdem einen Schritt des Spei-
cherns des ersten Codeschlüssels (SSN_1) in einem
internen Speicher des Prozessors des austausch-
baren Sicherheitsmoduls aufweist, sodass der er-
ste Codeschlüssel nicht beobachtet werden kann.

17. Decodierungsverfahren nach einem der Ansprüche
13 bis 16, das außerdem einen Schritt des Spei-
cherns des zweiten Codeschlüssels (SSN_1) in ei-
nem internen Speicher des Prozessors des festen
Sicherheitselements aufweist, sodass der zweite
Codeschlüssel nicht beobachtet werden kann.

18. Decodierungsverfahren nach einem der Ansprüche
13 bis 17, dadurch gekennzeichnet, dass

das feste Sicherheitselement ein erstes festes
Sicherheitselement eines Kabelnetzes ist, wo-
bei das Kabelnetz mindestens ein weiteres fe-
stes Sicherheitselement aufweist, und
der Schritt des Verarbeitens eines zweifach
chiffrierten Codeschlüssels den teildechiffrier-
ten Codeschlüssel erzeugt, sodass der teilde-
chiffrierte Codeschlüssel von keinem festen Si-
cherheitselement des mindestens einen weite-
ren festen Sicherheitselements als einfach chif-
frierter Codeschlüssel verarbeitet werden
kann, um den Arbeits-Codeschlüssel zu erzeu-
gen.

27   **EP 0 809 402 B1**   28

19. Ein Decodierungsverfahren in einem Decodierer mit den Schritten

Verarbeiten eines zweifach chiffrierten Codeschlüssels in einem Prozessor eines festen Sicherheitselements auf der Grundlage eines ersten Codeschlüssels (SSN_1), um einen teildechiffrierten Codeschlüssel zu erzeugen; Verarbeiten des teildechiffrierten Codeschlüssels in einem Prozessor eines austauschbaren Sicherheitsmoduls, das abanehmbar angebracht werden kann, als einfach chiffrierter Codeschlüssel (1061) auf der Grundlage eines zweiten Codeschlüssels (SSN_1), um einen Arbeits-Codeschlüssel (KOM1) zu erzeugen; und Verarbeiten von verschlüsselten Programmdaten (1062) auf der Grundlage des Arbeits-Codeschlüssels, um Decodierer-Kontrollinformationen (1058) zu erzeugen, die zum Entschlüsseln von verschlüsselten Signalen verwendet werden können.

20. Decodierungsverfahren nach Anspruch 19, das außerdem einen Schritt des Speicherns des Arbeits-Codeschlüssels in einem internen Speicher des Prozessors des austauschbaren Sicherheitsmoduls aufweist, sodass der Arbeits-Codeschlüssel nicht beobachtet werden kann.

21. Decodierungsverfahren nach Anspruch 19 oder 20, das außerdem einen Schritt des Speicherns des zweiten Codeschlüssels (SSN_1) in einem internen Speicher des Prozessors des austauschbaren Sicherheitsmoduls aufweist, sodass der zweite Codeschlüssel nicht beobachtet werden kann.

22. Decodierungsverfahren nach einem der Ansprüche 19 bis 21, das außerdem einen Schritt des Speicherns des ersten Codeschlüssels (SSN_1) in einem internen Speicher des Prozessors des festen Sicherheitselements aufweist, sodass der erste Codeschlüssel nicht beobachtet werden kann.

23. Decodierungsverfahren nach einem der Ansprüche 19 bis 22, das außerdem einen Schritt des Speicherns des zweiten Codeschlüssels (SSN_1) in einem internen Speicher des Prozessors des austauschbaren Sicherheitsmoduls aufweist, sodass der zweite Codeschlüssel nicht beobachtet werden kann.

24. Decodierungsverfahren nach einem der Ansprüche 19 bis 23, dadurch gekennzeichnet, dass

das austauschbare Sicherheitsmodul ein erstes austauschbares Sicherheitsmodul eines Kabelnetzes ist, wobei das Kabelnetz mindestens ein weiteres austauschbares Sicher-

heitsmodul aufweist, und der Schritt des Verarbeitens eines zweifach chiffrierten Codeschlüssels den teildechiffrierten Codeschlüssel erzeugt, sodass der teildechiffrierte Codeschlüssel von keinem austauschbaren Sicherheitsmodul des mindestens einen weiteren austauschbaren Sicherheitsmoduls als einfach chiffrierter Codeschlüssel verarbeitet werden kann, um den Arbeits-Codeschlüssel zu erzeugen.

25. Decodierungsverfahren nach einem der Ansprüche 13 bis 24, das außerdem einen Schritt des Wiederholens des Schritts des Verarbeitens von verschlüsselten Programmdaten aufweist, um aufeinander folgende Decodierer-Kontrollinformationen aus fortlaufend verarbeiteten verschlüsselten Programmdaten zu erzeugen, während der Arbeits-Codeschlüssel unverändert bleibt.

Revendications

1. Décodeur comprenant un élément de sécurité fixe (719), l'élément de sécurité fixe comprenant un processeur (713) pour traiter une clé cryptée une première fois (1061) sur la base d'une clé (SSN_0) pour générer une clé de travail (KOM1) et pour traiter des données de programme brouillé (1062) sur la base de la clé de travail afin de générer des informations de commande de décodeur (1058) utilisables pour désembrouiller des signaux brouillés, le décodeur comprenant en outre un module de sécurité remplaçable pouvant être fixé de façon amovible au décodeur, le module de sécurité remplaçable comprenant un processeur pour traiter une clé cryptée deux fois sur la base d'une seconde clé (SSN_1) afin de générer une clé partiellement décryptée, le processeur de l'élément de sécurité fixe traitant la clé partiellement décryptée en tant que clé cryptée une première fois de sorte que la clé de travail est récupérée à partir de la clé cryptée deux fois.

2. Décodeur selon la revendication 1, dans lequel le processeur de l'élément de sécurité fixe comprend un processeur sécurisé avec une mémoire interne afin de mémoriser la clé de travail et configuré de telle sorte que la clé de travail ne puisse pas être observée.

3. Décodeur selon la revendication 1 ou la revendication 2, dans lequel le processeur de l'élément de sécurité fixe comprend un processeur sécurisé avec un mémoire interne, afin de mémoriser la première clé (SSN_0) et configuré de manière à ce que la première clé ne puisse pas être observée.

4. Décodeur selon la revendication 1, 2 ou 3, dans le-

29   EP 0 809 402 B1   30

quel le processeur de l'élément de sécurité fixe est configuré pour générer les informations de commande de décodeur successives à partir de données de programme brouillé traitées de façon successive alors que la clé de travail reste inchangée.

5. Décodeur selon l'une quelconque des revendications 1 à 4, dans lequel le processeur du module de sécurité remplaçable comprend un processeur sécurisé avec une mémoire interne, afin de mémoriser la seconde clé (SSN_1) et configuré de manière à ce que la seconde clé ne puisse pas être observée.

6. Décodeur selon l'une quelconque des revendications 1 à 5, dans lequel le décodeur est un premier décodeur d'un système à câble, le système à câble comprenant au moins un autre décodeur, chaque décodeur dudit au moins un autre décodeur comprenant un élément de sécurité fixe associé, le module de sécurité remplaçable du premier décodeur étant incapable de générer une clé cryptée une première fois qui puisse être traitée par l'élément de sécurité fixe d'un décodeur quelconque dudit au moins un autre décodeur en vue de générer la clé de travail.

7. Décodeur comprenant un module de sécurité remplaçable (1014), le module de sécurité remplaçable comprenant un processeur (1051) destiné à traiter une clé cryptée une première fois (1061) sur la base d'une première clé (SSN_0) afin de générer une clé de travail (KOM1) et de traiter des données de programme brouillées (1062) sur la base de la clé de travail afin de générer des informations de commande de décodeur (1058) utilisables pour désembrouiller les signaux brouillés, le décodeur comprenant en outre un élément de sécurité fixe, l'élément de sécurité fixe comprenant un processeur pour traiter une clé cryptée deux fois sur la base d'une seconde clé (SSN_1), afin de générer une clé partiellement décryptée, le processeur du module de sécurité remplaçable traitant la clé partiellement décryptée en tant que clé cryptée une première fois de façon à ce que la clé de travail soit récupérée à partir de la clé cryptée deux fois.

8. Décodeur selon la revendication 7, dans lequel le processeur du module de sécurité remplaçable comprend un processeur sécurisé avec une mémoire interne, afin de mémoriser la clé de travail et configuré de manière à ce que la clé de travail ne puisse pas être observée.

9. Décodeur selon la revendication 7 ou 8, dans lequel le processeur du module de sécurité remplaçable comprend un processeur sécurisé avec une mémoire interne afin de mémoriser la première clé

(SSN_0) et configuré de manière à ce que la première clé ne puisse pas être observée.

10. Décodeur selon la revendication 7, 8 ou 9, dans lequel le processeur du module de sécurité remplaçable est configuré de façon à générer des informations de commande de décodeur successives à partir de données de programme brouillées traitées successivement alors que la clé de travail reste inchangée.

11. Décodeur selon l'une quelconque des revendications 7 à 10, dans lequel le processeur de l'élément de sécurité fixe comprend un processeur sécurisé avec une mémoire interne, afin de mémoriser la seconde clé (SSN_1) et configuré de manière à ce que la seconde clé ne puisse pas être observée.

12. Décodeur selon l'une quelconque des revendications 7 à 11, dans lequel le décodeur est un premier décodeur d'un système à câble, le système à câble comprenant au moins un autre décodeur, chaque décodeur dudit au moins un autre décodeur comprenant un module de sécurité remplaçable associé, l'élément de sécurité fixe du premier décodeur étant incapable de générer une clé cryptée une première fois qui puisse être traitée par le module de sécurité remplaçable d'un décodeur quelconque dudit au moins un autre décodeur afin de générer la clé de travail.

13. Procédé de décodage dans un décodeur, comprenant les étapes consistant à :

traiter une clé cryptée deux fois dans un processeur d'un module de sécurité remplaçable pouvant être fixé de façon amovible sur la base d'une première clé (SSN_1) afin de générer une clé partiellement décryptée, traiter la clé partiellement décryptée dans un processeur d'un élément de sécurité fixe en tant que clé cryptée une première fois (1061) sur la base d'une seconde clé (SSN_0) afin de générer une clé de travail (KOM1), et traiter des données de programme brouillées (1062) sur la base de la clé de travail afin de générer des informations de commande de décodeur (1058) utilisables pour désembrouiller des signaux brouillés.

14. Procédé de décodage selon la revendication 13, comprenant en outre une étape consistant à mémoriser la clé de travail dans une mémoire interne du processeur de l'élément de sécurité fixe de manière à ce que la clé de travail ne puisse pas être observée.

15. Procédé de décodage selon la revendication 13 ou

31   EP 0 809 402 B1   32

la revendication 14, comprenant en outre une étape consistant à mémoriser la seconde clé (SSN_0) dans une mémoire interne du processeur de l'élément de sécurité fixe de manière à ce que la seconde clé ne puisse pas être observée.

16. Procédé de décodage selon l'une quelconque des revendications 13 à 15, comprenant en outre une étape consistant à mémoriser la première clé (SSN_1) dans une mémoire interne du processeur du module de sécurité remplaçable de manière à ce que la première clé ne puisse pas être observée.

17. Procédé de décodage selon l'une quelconque des revendications 13 à 16, comprenant en outre une étape consistant à mémoriser la seconde clé (SSN_0) dans une mémoire interne du processeur de l'élément de sécurité fixe de manière à ce que la seconde clé ne puisse pas être observée.

18. Procédé de décodage selon l'une quelconque des revendications 13 à 17, dans lequel :

l'élément de sécurité fixe est un premier élément de sécurité fixe d'un système à câble, le système à câble comprenant au moins un autre élément de sécurité fixe, et
l'étape de traitement d'une clé cryptée deux fois génère la clé partiellement décryptée de manière à ce que la clé partiellement décryptée ne puisse pas être traitée en tant que clé cryptée une première fois par tout élément de sécurité fixe quelconque du au moins un autre élément de sécurité fixe en vue de générer la clé de travail.

19. Procédé de décodage dans un décodeur comprenant les étapes consistant à :

traiter une clé cryptée deux fois d'un processeur d'un élément de sécurité fixe sur la base d'une première clé (SSN_1) afin de générer une clé partiellement décryptée,
traiter la clé partiellement décryptée dans un processeur d'un module de sécurité remplaçable pouvant être fixé de façon amovible en tant que clé cryptée une première fois (1061) sur la base d'une seconde clé (SSN_0) afin de générer une clé de travail (KOM1), et
traiter des données de programme brouillées (1062) sur la base de la clé de travail afin de générer des informations de commande de décodeur (1058) utilisables pour le désembrouillage des signaux brouillés.

20. Procédé de décodage selon la revendication 19, comprenant en outre une étape consistant à mémoriser la clé de travail dans une mémoire interne du

processeur du module de sécurité remplaçable de manière à ce que la clé de travail ne puisse pas être observée.

21. Procédé de décodage selon la revendication 19 ou la revendication 20, comprenant en outre une étape consistant à mémoriser la seconde clé (SSN_0) dans une mémoire interne du processeur du module de sécurité remplaçable de manière à ce que la seconde clé ne puisse pas être observée.

22. Procédé de décodage selon l'une quelconque des revendications 19 à 21, comprenant en outre une étape consistant à mémoriser la première clé (SSN_1) dans une mémoire interne du processeur de l'élément de sécurité fixe de manière à ce que la première clé ne puisse pas être observée.

23. Procédé de décodage selon l'une quelconque des revendications 19 à 22, comprenant en outre une étape consistant à mémoriser la seconde clé (SSN_0) dans une mémoire interne du processeur du module de sécurité remplaçable de manière à ce que la seconde clé ne puisse pas être observée.

24. Procédé de décodage selon l'une quelconque des revendications 19 à 23, dans lequel :

le module de sécurité remplaçable est un premier module de sécurité remplaçable d'un système à câble, le système à câble comprenant au moins un autre module de sécurité remplaçable, et
l'étape de traitement de la clé cryptée deux fois génère la clé partiellement décryptée de manière à ce que la clé partiellement décryptée ne puisse pas être traitée en tant que clé cryptée une première fois par un module de sécurité remplaçable quelconque du au moins un autre module de sécurité remplaçable en vue de générer la clé de travail.

25. Procédé de décodage selon l'une quelconque des revendications 13 à 24, comprenant en outre une étape consistant à répéter l'étape de traitement des données de programme brouillées afin de générer des informations de commande de décodeur successives provenant de données de programme brouillées traitées successivement alors que la clé de travail reste inchangée.
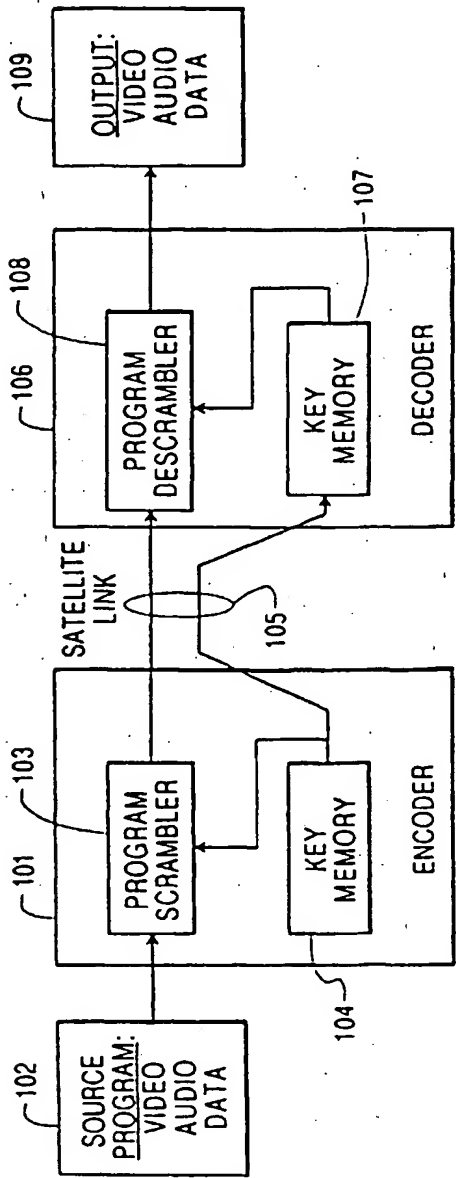
5

10

15

20

25

30

35

40

45

50

55

EP 0 809 402 B1

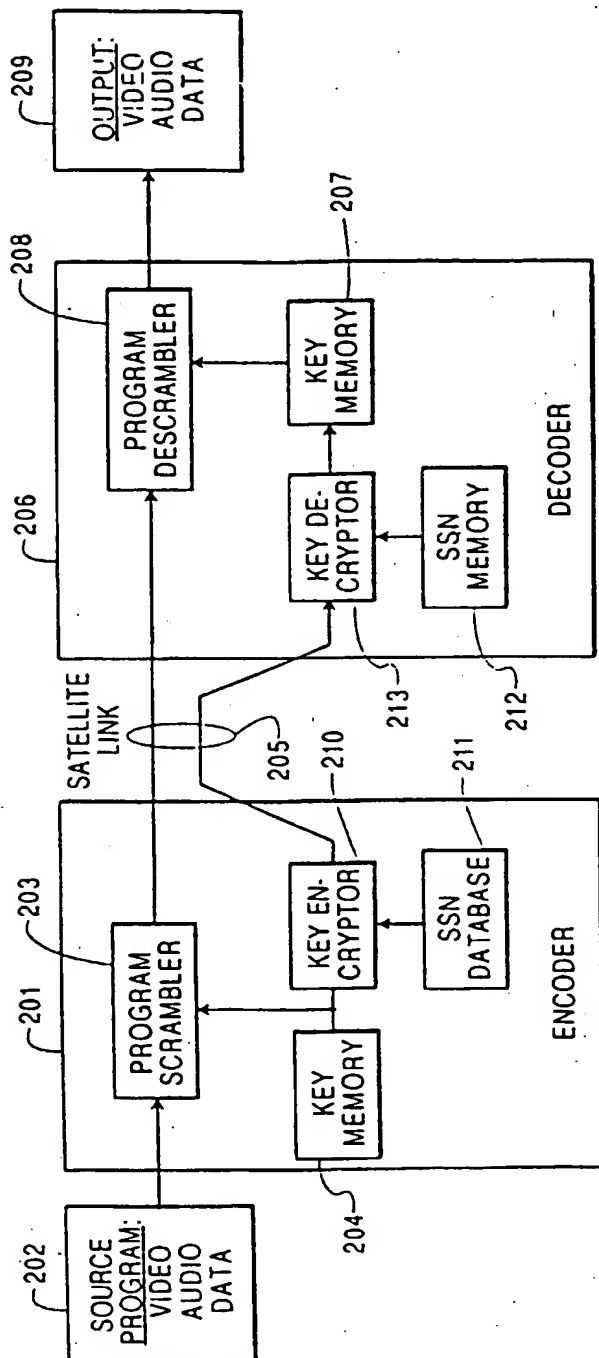**FIG. 1**
PRIOR ART
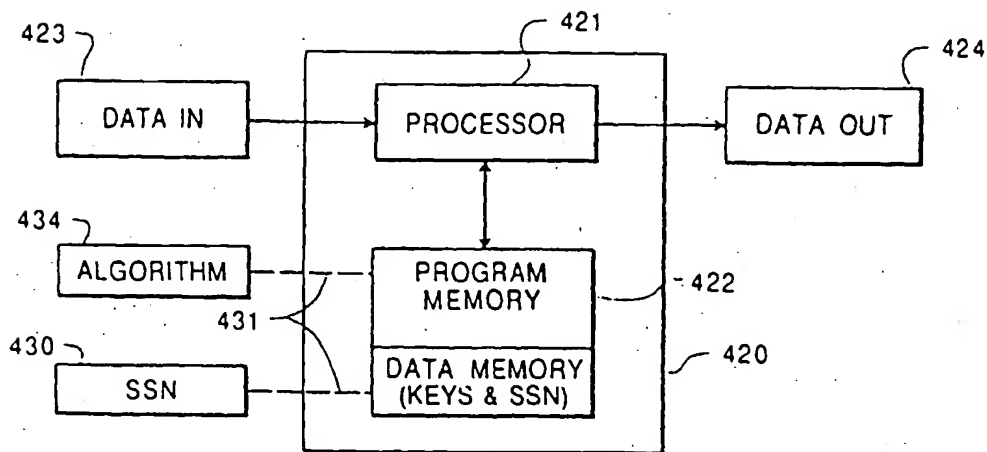
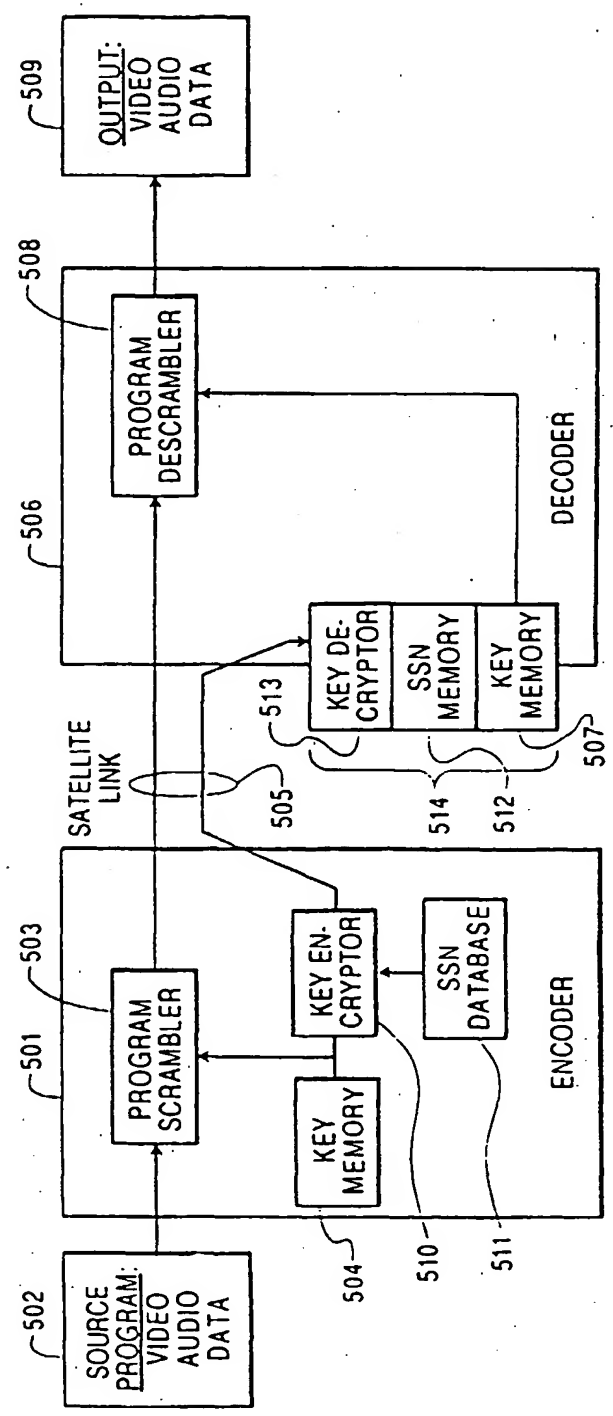EP 0 809 402 B1

FIG. 2
PRIOR ART

EP 0 809 402 B1

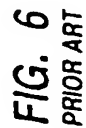323 — DATA IN → PROCESSOR — 321 → DATA OUT — 324

325 — MEMORY ADDRESS   328 → PROGRAM MEMORY — 327 → MEMORY DATA — 326

320   322

FIG. 3
PRIOR ART

423 — DATA IN → PROCESSOR — 421 → DATA OUT — 424

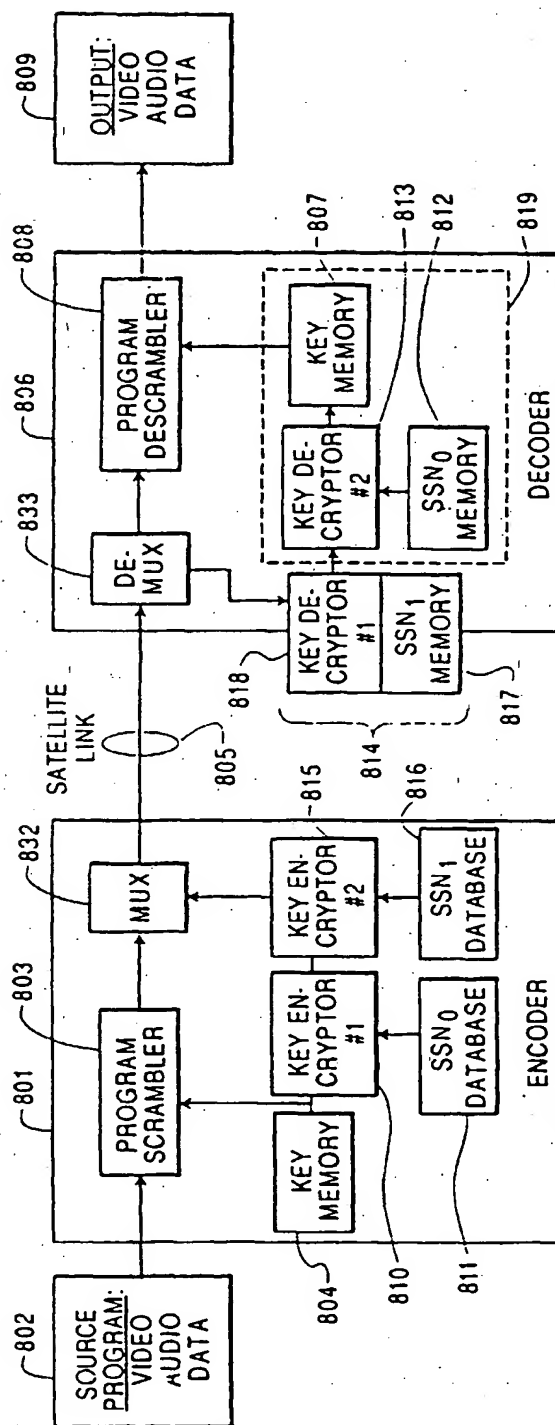434 — ALGORITHM   PROGRAM MEMORY — 422
431
430 — SSN   DATA MEMORY (KEYS & SSN) — 420

FIG. 4

EP 0 809 402 B1

FIG. 5

EP 0 809 402 B1

FIG. 6
PRIOR ART
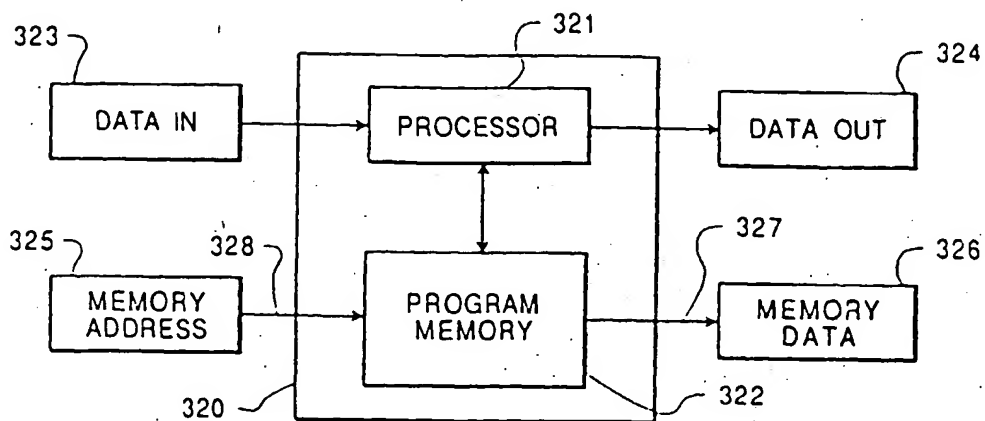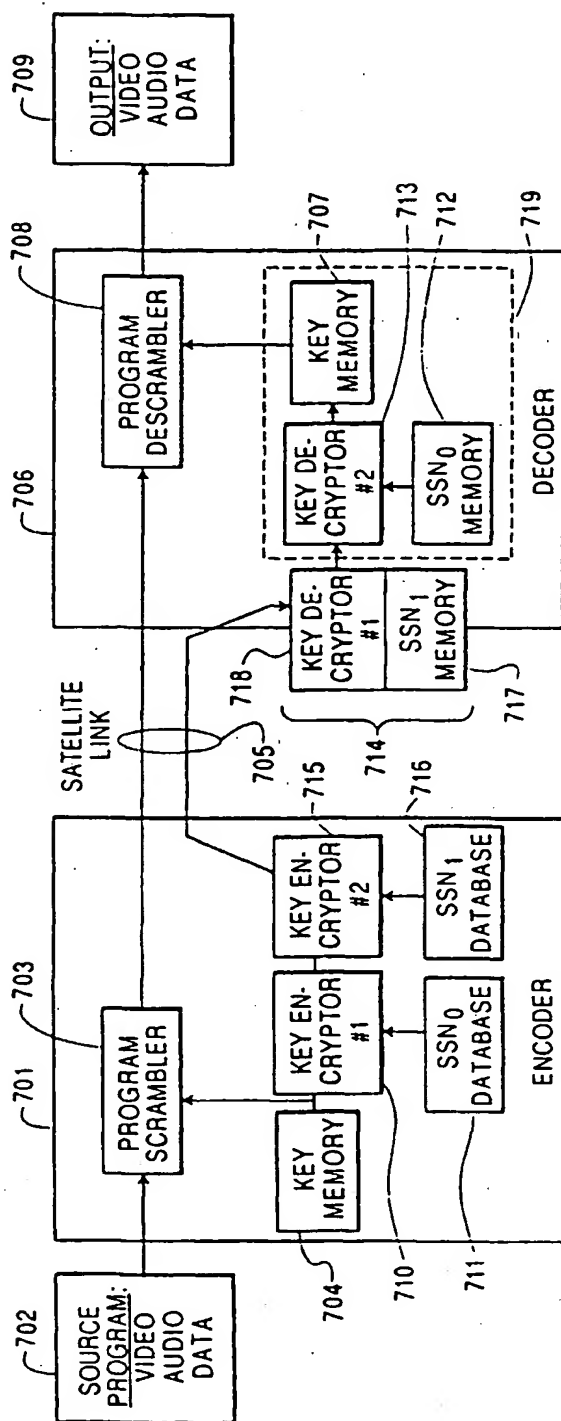
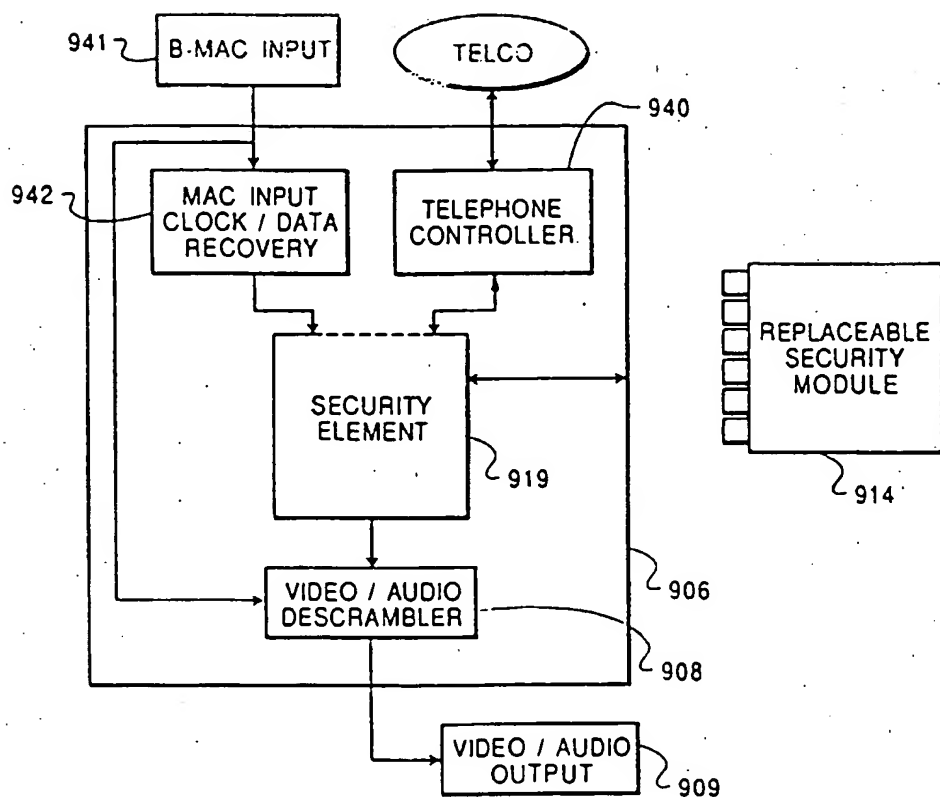EP 0 809 402 B1

FIG. 7

EP 0 809 402 B1

FIG. 8

EP 0 809 402 B1

FIG. 9

EP 0 809 402 B1

FIG. 10

FIG. 11